CLAIMS

I claim:

1. A method for processing a policy-lookup for network protection by employing a policy table comprising a plurality of policy-table entries PTE(ip), where ip= 1, 2, 3, ...N and N is a positive integer representing a total number of said PTE(ip), with each PTE(ip) comprising data for defining a plurality of destination address ranges between a first destination address DA1(ip) and a second destination address DA2(ip), a source address ranges between a first source address SA1(ip) and second source address SA(ip), a destination port group ranging between a first destination port DP1(ip) and second destination port DP2(ip) and a source port group ranging between a first source port SP1(ip) and a second source port SP2(ip), said method comprising steps of:

generating an array of destination address segments by arranging ranges represented by {DA1(ip), DA2(ip)}, for ip=1, 2, 3, ...N, according to a destination address sequential order thus generating a plurality of destination address segments S1(Idas) between first destination address A11(Idas) and second destination address A12(Idas) where Idas is a series of destination address sequence number (DASN) and Idas=1, 2, 3, ...IIdas, and IIdas is a positive integer less than or equal to 2N-1;

generating an array of source address segments by arranging ranges represented by {SA1(ip), SA2(ip)}, for ip=1, 2, 3, ...N, according to a source address sequential order thus generating a plurality of source address segments S2(Isas) between a first source address A21(Isas) and a second source address A22(Isas), where Isas is a series of source address sequence number (SASN) and Isas=1, 2, 3, ...IIsas, and IIsas is a positive integer less than or equal to 2N-1;

forming a source-destination address mapping table (SDAMT) comprising a plurality of SDAMT table entries SDA(Isas, Idas) with Isas=1, 2, 3, ...IIsas, and Idas=1, 2, 3, ...IIdas and SD(Isas, Idas)=ip1 wherein ip1 is a policy-table entry counter of a first policy table entry wherein said S2(Isas) is included a range defined by SA1(ip1) and SA2(ip1), and said S1(Idas)is included in a range defined by DA1(ip1), DA2(ip1);

generating an array of destination port segments by arranging ranges represented by {DP1(ip), DP2(ip)}, for ip=1, 2, 3, ...N, according to a destination address sequential order thus generating a plurality of destination address segments P1(Idps) between a first destination port P11(Idps) and a second destination port P12(Idps), where Idps is a series of destination port sequence number (DPSN) and Idps=1, 2, 3, ...IIdps, and IIdps is a positive integer less than or equal to 2N-1;

generating an array of source port segments by arranging ranges represented by {SP1(ip), SP2(ip)}, for ip=1, 2, 3, ...N, according to a source address sequential order thus generating a plurality of source address segments S2(Isps) between a first source port P21(Isps) and a second source port P22(Isps), where Isps is a series of source address sequence number (SPSN) and Isps=1, 2, 3, ...IIsps, and IIsps is a positive integer less than or equal to 2N-1; and

forming a source-destination port mapping table (SDPMT) comprising a plurality of SDPMT table entries SDP(Isps, Idps) with Isps=1, 2, 3, ...IIsps, and Idps=1, 2, 3, ...IIdps and SDP(Isps, Idps)=ip2 wherein ip2 is a policy-table entry counter of a first policy table entry wherein said S2(Isps) is included a range defined by SP1(ip2) and SP2(ip2), and said S2(Idps)is included in a range defined by DP1(ip2), DP2(ip2).

2. The method of claim 1 further comprising steps of:

forming a policy mapping table by generating a policy-mapping table entry PMT(ip, ip) for ip= 1, 2, 3,…,N, wherein PMT(ip3, ip4) = ip for ip = 1, 2, 3, …,N and ip3= ip1(R1), and ip4=ip2(R2), and ip1(R1) representing all policy-table entry counters in said SDAMT within a two-dimensional range defined by {SA1(ip), SA2(ip)} and {DA1(ip), DA2(ip)}, and ip2(R2) representing all policy-table entry counters in said SDPMT within a two-dimensional range defined by {SP1(ip), SP2(ip)} and {DP1(ip), DP2(ip)}.

3. The method of claim 1 further comprising steps of:

forming a destination address binary tree by generating an array of tree elements each having a root destination-address and two branch destination addresses and recursively each root destination address is further assigned as a next level root destination address for generating two next-level branch destination addresses wherein a first root address is A11(R1) where R1 =N/2 if N is an even number and R1 is (N+1)/2 if N is an odd number, and said two branch destination addresses are A12(R1-1) and A12(R1);

forming a source address binary tree by generating an array of tree elements each having a root source-address and two branch destination addresses and recursively each root destination address is further assigned as a next level root destination address for generating two next-level branch destination addresses wherein a first root address is A21(R1) and said two branch destination addresses are A22(R1-1) and A22(R1);

forming a destination port binary tree by generating an array of tree elements each having a root destination-port and two branch destination ports and recursively each root destination port is further assigned as a next level root destination port for generating two next-level branch destination port wherein a first root address is P11(R1) and said two branch destination ports are P12(R1-1) and P12(R1); and

forming a source port binary tree by generating an array of tree elements each having a root source-port and two branch source ports and recursively each root source port is further assigned as a next level root source port for generating two next-level branch source port wherein a first root address is P21(R1) and said two branch destination ports are P22(R1-1) and P22(R1).

4. The method of claim 3 further comprising steps of:

receiving an incoming packet containing data for parsing a designated destination and source addresses represented by DDA and DSA respectively, and a designated destination and source ports represented by DDP and DSP respectively; and

searching along said destination address binary tree for determining a destination address root DAR and a destination address branch DAB wherein DAB<DDA<DAR and determining a destination address sequence number DASN(DDA) for said DDA;

searching along said source address binary tree for determining a source address root SAR and a source address branch SAB wherein SAB<DSA<DAR and determining a source address sequence number SASN(DSA) for said DSA;
searching along said destination port binary tree for determining a destination port root DPR and a destination port branch DPB wherein DPB<DDP<DPR and determining a destination port sequence number DPSN(DDP) for said DDP;

searching along said source port binary tree for determining a source port root SPR and a source port branch SPB wherein SPB<DSP<DPR and determining a source port sequence number SPSN(DSP) for said DSP; and

applying said DASN(DDA), SASN(DSA), DPSN(DDP), and SPSN(DSP) for search said SDAMT, SDPMT, and PMT for finding a policy table entry counter ip for receiving said incoming packet only when a policy-table entry counter ip is found from said PMT.

5. A method for processing a policy table comprising a plurality of policy-table entries with each entry comprising data for defining a plurality of destination address ranges, a source address ranges, a destination port group and a source port group, said method comprising steps of:

assigning an ordered sequence number as a policy-table entry counter ip to each of said policy table entries;

fragmenting said destination address ranges and said source address ranges listed in said policy table entries into a plurality of a sequentially-ordered destination address segments and source address segments respectively and each segment is assigned with a sequential segment number thus generating a set of source address sequence numbers (SASN) and a set of destination address sequence numbers (DASN);

forming a source-destination address mapping table (SDAMT) comprising a plurality of SDAMT table entries for each pair of SASN and DASN wherein each of said SDAMT table entries is provided with a policy-table entry counter ip corresponding to a first policy table entry wherein said SASN and DASN being listed;

fragmenting said destination port groups and said source port groups listed in said policy table entries into a plurality of a sequentially-ordered destination port segments and source port segments respectively and each segment is assigned with a sequential segment number thus generating a set of source port sequence numbers (SPSN) and a set of destination port sequence numbers (DPSN); and

forming a source-destination port mapping table (SDPMT) comprising a plurality of SDPMT table entries for each pair of SPSN and DPSN wherein each of said SDPMT table entries is provided with a policy-table entry counter ip corresponding to a first policy table entry wherein said SPSN and DPSN being listed.

6. A method for processing a table comprising a plurality of table entries with each entry defined data for defining a plurality of multiple-dimensional spaces, said method comprising steps of:

assigning an ordered sequence number as a table entry counter ip to each of said table entries;

fragmenting said multiple-dimensional spaces into order spatial ranges and assigned each of said spatial ranges with a sequential spatial range-numbers;

forming multiple-dimensional range-spaces by employing said sequential spatial range-numbers as coordinates and assigning an associated table entry counter ip to each block defined by said spatial range-number coordinates for providing an index for correlating each of said sequential spatial range-numbers to said each of said table entry.

7. The method of claim 6 further comprising steps of:

forming a multiple dimensional table-entry counter space defined by table-entry counters as coordinates wherein a spatial space defined by said coordinates and pointed by a combination of all of said associated table entry counter ipc entered into each of said multiple-dimensional range spaces associated with said counter ip is entered with a value of a table entry counter ip.

8. A database for use in processing a table wherein said table including a plurality of table entries each assigned with an ordered table entry counter ip and each entry defined data for defining a plurality of multiple-dimensional spaces, said database comprising:

an array of ordered spatial ranges each assigned with an ordered spatial range number generated from fragmenting said multiple-dimensional spaces into said array of order spatial ranges;

a multiple-dimensional table generated from forming a plurality of multiple-dimensional range-spaces by employing said sequential spatial range-numbers as coordinates and assigning an associated table entry counter ip to each block defined by said spatial range-number coordinates for providing an index for correlating each of said sequential spatial range-numbers to said each of said table entry.